



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,562	10/28/2005	Takehiko Nakano	266812US6PCT	6309
22850	7590	08/13/2009		
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314				
EXAMINER				
SHOLEMAN, ABUS				
ART UNIT		PAPER NUMBER		
2437				
NOTIFICATION DATE		DELIVERY MODE		
08/13/2009		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com

oblonpat@oblon.com

jgardner@oblon.com

Office Action Summary

Application No.

10/528,562

Applicant(s)

NAKANO ET AL.

Examiner

ABU SHOLEMAN

Art Unit

2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 May 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SI/309)
Paper No(s)/Mail Date 06/05/2009
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Response to Amendment

1. Claims 1-4, 6-14, 16-19, 21-23, 25, and 26 are pending in this application. Claims 1-4, 9, 14, 16, 18, 19, 21-23, and 26 are amended by the present amendment.
2. Applicant's arguments, see pages 17-23, filed 05/19/2009, with respect to the rejection(s) of claim(s) 1-4, 6-14, 16-19, 21-23, 25, and 26 under 35 U.S.C § 103(a) have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.
4. Claims 1-4, 16-19, 21-23, and 25-26 are rejected under 35 U.S.C 103(a) as being unpatentable over Haverinen et al (US 2002/0012433) (hereinafter Haverinen) in view of Rofheart et al (US 7058414) (hereinafter Rofheart) and further in view of Willey (US 2003/0065918) (hereinafter Willey).

As per claim 1, Haverinen discloses " a data transmitting apparatus comprising: "a command transmission transmitting unit configured to transmit a response request command to a data receiving apparatus" as (par 0177, and Fig .2, MT [transmitting unit] sends request extension [response request command] to PAC [data receiving apparatus]); "a control unit configured to receive a response message to the response request command from the data receiving apparatus" as (par 0177-0187, and Fig.2, MT received a n***RAND**,**SIGNrand** [response message] from PAC [data receiving apparatus] for request extension [response request command]);" the response message including authentication data based on shared data shared with said data receiving apparatus" as (par 0177-0187, and Fig.2, a n* **RAND**,**SIGNrand** [response message] include **SIGNrand** [authentication data] based on **MN_RAND** [shared data] with PAC[data receiving apparatus]); "an expected value generation unit configured to generate an expected authentication value based on the shared data" as (par 0177-0187, and Fig.2, MT calculate **SIGNrand** [expected authentication value] based on **MN_RAND** [Shared data] similarly as GAGW); "an authentication unit configured to produce an authentication result for said data receiving apparatus based on the expected value and said authentication data in the response message" as (par 0177-0187, and Fig.2, MT configured to produce a validation for PAC [data receiving apparatus] based on **SIGNrand** [authentication data]).

But Haverinen expressly fails to disclose " an expected value generation unit configured to generate an expected authentication value based on a sequence number, the sequence number indicating a position of the response request command in a

sequence of response request commands to be transmitted by the command transmission unit, a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message; and a judgment whether unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time".

However Rofheart discloses "a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message" as (Fig 7,numeral 713, compute round Trip time from transmitter to receiver, transmitter send a message at time t_1 [numeral 703] and transmitter received a response message from remote device at time t_2 [numeral 709] , response time $Trt=t_2-t_1-d$); "and a judgment whether unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time" as (Broader interpretation, column 4, line 22-35, enabling communications between local device with remote device depending on whether the distance [response time] satisfies authentication criteria [authentication result] , [e.g, response time satisfies authentication criteria]).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission based on authentication.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a

device authentication with response time that is taught by Rofheart because it would provide secure communication with a specific subscriber .

The combination of Haverinen and Rofheart fail to disclose an expected value generation unit configured to generate an expected authentication value based on a sequence number, the sequence number indicating a position of the response request command in a sequence of response request commands to be transmitted by the command transmission unit.

However, Willey discloses an expected value generation unit configured to generate an expected authentication value based on a sequence number, the sequence number indicating a position of the response request command in a sequence of response request commands to be transmitted by the command transmission unit (par 0072, and Fig.11, each device generate antispoof value [expected authentication value] based on a bit of value [sequence number] , a bit of the device 's antispoof variable based device's address).

Haverinen in view of Rofheart and Willey are analogous arts because they are same field of endeavor of the method for data transmission based on authentication.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen in view of Rofheart by including each device generate antispoof value [expected authentication value] based on a bit of value [sequence number], a bit of the device's antispoof variable based device's address that is taught by Willey because it would improved the security for a distance receiver.

As per claim 2, Haverinen in view of Rofheart in view of Willey " wherein: said command transmission unit is further configured to transmit said response request command a maximum of N times" as (Haverinen, paragraph 0038, and Fig.2, request for each session); "said control unit is further configured to receive the response messages from the data receiving apparatus for each of the N transmitted response request commands" as (Haverinen , par 0177-0187, and Fig.2, MT received a n*RAND,SIGNrand [response message] from PAC [data receiving apparatus] for request extension [response request command] for each session); and "said authentication unit is further configured to produce authentication results based on said authentication data in each received response message" as (Haverinen , par 0177-0187, and Fig.2, MT configured to produce a validation for PAC [data receiving apparatus] based on SIGNrand [authentication data]) .

As per claim 3, this claim is directed to a data transmission method and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 4, this claim is directed to a computer program and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 16, this claim is directed to an information transmitting apparatus and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 17, this claim is directed to an information transmitting apparatus and contains limitations that are substantially similar to those recited in claim 2 above, and accordingly is rejected for similar reasons.

As per claim 18, this claim is directed to a data transmission method and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 19, this claim is directed to a computer program and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 21, this claim is directed to a data receiving apparatus and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 22, this claim is directed to a data reception method and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 23, this claim is directed to a computer program and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

As per claim 25, Haverinen discloses A communication system comprising:

“a data transmitting apparatus (Fig .2, MT data transmitting apparatus) including,

a command transmission unit configured to transmit a response request command to a data receiving apparatus(par 0177, and Fig .2, MT [transmitting unit] sends request extension [response request command] to PAC [data receiving apparatus]) ,

a control unit configure to receive a response message to the response request command from the data receiving apparatus(par 0177-0187, and Fig.2, MT received a n***RAND**,SIGNrand [response message] from PAC [data receiving apparatus] for request extension [response request command]), the response message including authentication data based on shared data shared with said data receiving apparatus(par 0177-0187, and Fig.2, a n* **RAND**,SIGNrand [response message] include SIGNrand [authentication data] based on MN_ **RAND** [shared data] with PAC[data receiving apparatus]) ,

an expected value generation unit configured to generate an expected authentication value based on the shared data (par 0177-0187, and Fig.2, MT calculate SIGNrand [expected authentication value] based on MN_RANDOM [Shared data] similarly as GAGW),

an authentication unit configured to produce an authentication result for said data receiving apparatus based on the expected value and said authentication data (par 0177-0187, and Fig.2, MT configured to produce a validation for PAC [data receiving apparatus] based on SIGNrand [authentication data]),

the data receiving apparatus configured to receive data from the data transmitting apparatus (Fig.2 , PAC-GAGW is configured to receive data from MT data transmitting apparatus), the data receiving apparatus including

a command receiving unit configured to receive the response request command from the data transmitting apparatus (par 0177, and Fig .2, MT [transmitting unit] sends request extension [response request command] to PAC [data receiving apparatus]),

“an authentication data generation unit configured to generate said authentication data based on the shared data by subjecting said shared data to a predetermined process before said response request command is received from said data transmitting apparatus” as (par 0177-0187, and Fig .2, PAC-GAGW generated SIGNrand [authentication data] based on MN_RANDOM [shared data] with MT[data transmitting apparatus] and MN_RANDOM [shared data] is randomly produced before request extension [response request command] is received from MT [data transmitting

apparatus] , MN RAND is generated first then send a Request extension to PAC_GAGW [data receiving apparatus]);

“a response message generation unit configured to generate the response message to said response request command before said response request command is received from said data transmitting apparatus (par 0177-0187 , par 0170 and par 0211 and Fig .2, A singer response SRES which is generated in MSC before a request [MN RAND] arrived at PAC-GAGW. MSC randomly pre -produced SRES based on RAND number, not from MN RAND request command, A GSM triplet [RAND, Kc, SRES] is already generated in MSC before any signer form MT [data transmitting unit] , It is showing at Fig. 2, PAC_GAGW get SRES after request arrived at PAC, but SRES is already created at MSC based on RAND, broader interpretation, it would be RAND is generated at MSC before MN RAND arrived at PAC-GAGW, PAC-GAGW sends n RAND, SIGNrand [response message] to MT [data transmitting apparatus]) , said response message including said authentication data” as (par 0177-0187, and Fig .2, PAC-GAGW sends n RAND, SIGNrand [response message] to MT [data transmitting apparatus] with SIGNrand [authentication data]), and

a transmission unit configured to transmit said response message to said data transmitting apparatus when said response request command is received from said data transmitting apparatus” as (par 0177-0187, and Fig .2, PAC-GAGW transmits n RAND, SIGNrand [response message] when request command (MN RAND) is received from MT [data transmitting apparatus]).

But Haverinen expressly fails to disclose "a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message, and

a judgment unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time.

However Rofheart discloses "a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message" as (Fig 7,numeral 713, compute round Trip time from transmitter to receiver, transmitter send a message at time t_1 [numeral 703] and transmitter received a response message from remote device at time t_2 [numeral 709] , response time $Trt=t_2-t_1-d$), and "a judgment unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time" as (Broader interpretation, column 4, line 22-35, enabling communications between local device with remote device depending on whether the distance [response time] satisfies authentication criteria [authentication result] , [e.g, response time satisfies authentication criteria]).

Haverinen and Rofheart are analogous arts because they are same field of endeavor of the method for data transmission based on authentication.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a

device authentication with response time that is taught by Rofheart because it would provide secure communication with a specific subscriber .

As per claim 26, this claim is directed to a communication system and contains limitations that are substantially similar to those recited in claim 1 above, and accordingly is rejected for similar reasons.

5. Claims 6- 14 are rejected under 35 U.S.C 103(a) as being unpatentable over Haverinen et al (US 2002/0012433) (hereinafter Haverinen) in view of Rofheart et al (US 7058414) (hereinafter Rofheart)

As per claim 6, Haverinen discloses "a data receiving apparatus comprising: a command receiving unit configured to receive the response request command from the data transmitting apparatus" as (par 0177, and Fig .2, MT [transmitting unit] sends request extension [response request command] to PAC [data receiving apparatus]); " an authentication data generation unit configured to generate said authentication data based on shared data shared with the data transmitting apparatus by subjecting said shared data to a predetermined process before said response request command is received from said data transmitting apparatus" as (par 0177-0187, and Fig .2, PAC-GAGW generated SIGNrand [authentication data] based on MN_RANDOM [shared data] with MT[data transmitting apparatus] and MN_RANDOM [shared data] is randomly produced before request extension [response request command] is received from MT

[data transmitting apparatus] , MN RAND is generated first then send a Request extension to PAC GAGW [data receiving apparatus] ; "a response message generation unit configured to generate the response message to said response request command before said response request command is received from said data transmitting apparatus" as (par 0177-0187 , par 0170 and par 0211 and Fig .2, A singer response SRES which is generated in MSC before a request [MN RAND] arrived at PAC-GAGW. MSC randomly pre -produced SRES based on RAND number, not from MN RAND request command, A GSM triplet [RAND, Kc, SRES] is already generated in MSC before any signer form MT [data transmitting unit] , It is showing at Fig. 2, PAC GAGW get SRES after request arrived at PAC, but SRES is already created at MSC based on RAND, broader interpretation, it would be RAND is generated at MSC before MN RAND arrived at PAC-GAGW, PAC-GAGW sends n RAND, SIGNrand [response message] to MT [data transmitting apparatus]), "said response message including said authentication data" as (par 0177-0187, and Fig .2, PAC-GAGW sends n RAND, SIGNrand [response message] to MT [data transmitting apparatus] with SIGNrand [authentication data]) and

"a transmission unit configured to transmit said response message to said data transmitting apparatus when said response request command is received from said data transmitting apparatus" as (par 0177-0187, and Fig .2, PAC-GAGW transmits n RAND, SIGNrand [response message] when request command (MN RAND) is received from MT [data transmitting apparatus]).

But Haverinen expressly fails to disclose "A data receiving apparatus with configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on authentication data and response time between sending a response request command and receiving a response message.

However Rofheart discloses "A data receiving apparatus with configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on authentication data and response time between sending a response request command and receiving a response message" as (Broader interpretation, column 4, line 22-35, enabling communications between local device with remote device depending on whether the distance [response time] satisfies authentication criteria [authentication result] , [e.g, response time satisfies authentication criteria]).

Haverinen in view of Rofheart and Willey are analogous arts because they are same field of endeavor of the method for data transmission based on authentication.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Haverinen by including a device authentication with response time that is taught by Rofheart because it would provide a secure communication with a specific subscriber via challenge-response.

As per claim 7,Haverinen in view Rofheart discloses " said shared data is a quasi random number" as (Haverinen, paragraph 0037, the challenge are random);

"transmitted from said data transmitting apparatus before said response request command is transmitted" as (Haverinen, claim 0170, the challenge sent before response are received from the SIM); and" said authentication data generation Unit is further configured to subject said quasi random number to a Keyed-Hash process to produce a Hash value that is used as said authentication data " as (Haverinen, paragraph 0180 and Fig 2, hash value is calculated from random value in the authentication unit).

As per claim 8, Haverinen in view Rofheart discloses "wherein: said authentication data generation unit is further configured to execute a Keyed-Hash process relative to said quasi random number and information specific to the information processing apparatus to produce a Hash value that is used as said authentication data" as (Haverinen, paragraph 0187 and Fig 2, authentication is complete and the FAAA and the MT share k and K is calculated by hashing the random).

As per claim 9, Haverinen in view Rofheart discloses " that wherein: said command receiving unit is further configured to receive said response request command from said data transmitting apparatus a maximum of N times" as (Haverinen, Fig 2, N times of command are transmitted from MT to PAC); said" authentication data generation unit is further configured to execute said predetermined process relative to said shared data before a first one of said response request command commands is received from said data transmitting apparatus and further configured to generate N

sets of said authentication data corresponding to said N received response request Commands" as (Haverinen, Fig 2, authentication is done on shared data. Each packet gets authenticated in each session); and "said transmission unit is further configured to transmit said response message generated by said response message generation unit to said data transmitting apparatus, said response message including the N sets of said authentication data in a sequence agreed beforehand with said data transmitting apparatus" as (Haverinen, Fig 2. PAC sends response of N number of N packet data to MT after authentication).

As per claim 10, Haverinen in view Rofheart discloses "wherein: said authentication data generation unit is further configured to divide the data obtained by subjecting said shared data to said process into a plurality of data pieces and further configured to generate the N sets of said authentication data from the divided data" as (Haverinen, Fig 2, it is obvious that packet data is division of whole data. GAGW authenticate each packet of data).

As per claim 11, Haverinen in view Rofheart discloses: "wherein: said authentication data generation means unit is further configured to generate the N sets of said authentication data based on data obtained at each process of repetitively executing said predetermined process relative to said shared data" as (Haverinen, Fig 2, GAGW authenticate to the sequence of the packet data) .

As per claim 12, Haverinen in view Rofheart discloses wherein: said transmission unit is further configured to transmit the response message to said

transmitting apparatus when said response request command is received from the data transmitting apparatus, said response message containing new authentication data generated from said authentication data and information contained in said response request command" as (Haverinen, Fig 2, GAGW transmits authentication information to PAC. When GAGW send response to PAC, Each authenticated data with the new authentication key).

As per claim 13, this claim is directed to a data reception method and contains limitations that are substantially similar to those recited in claim 6 above, and accordingly is rejected for similar reasons.

As per claim 14, this claim is directed to a computer program and contains limitations that are substantially similar to those recited in claim 6 above, and accordingly is rejected for similar reasons.

Examiner Notes

6. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abu Sholeman whose telephone number is (571)270-7314 and Fax number is (571)-270-8314. The examiner can normally be reached on Monday through Thursday 9:30 AM - 6:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ABU SHOLEMAN/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437